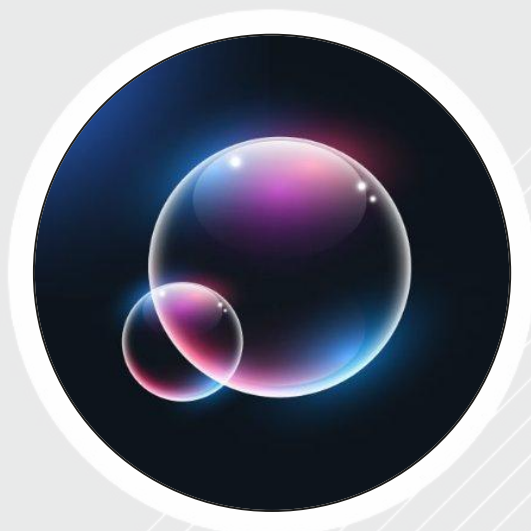# SPYWOLF

Security Audit Report

(TESTNET)

Completed on
May 24, 2023

OVERVIEW

This audit has been prepared for **BLOOMBLOCK** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> – SPYWOLF Team –

TABLE OF CONTENTS

BLOOMBLOCK

PROJECT DESCRIPTION

According to their whitepaper:

BloomBlock.News is a Crypto focused news source for users to streamline their research on the Blockchain. This includes articles and videos to inform users on general crypto news. Track your favourite Crypto currencies with our real-time live price index while staying up to date on market trends and updates.

Articles and Tweets are automatically posted for a fast, accurate and unbiased update. A growing user base will be monetized with affiliate and sponsorship advertising to grow exposure. Accumulated verified news platforms are linked to BloomBlock for articles to be uploaded for fast, accurate and unbiased Blockchain news.

Release Date: Presale starts in May, 2023

Category: DeFi

01

CONTRACT INFO

Token Name
BLOOMBLOCK

Symbol
BLOOM

Contract Address
0x40a43e1F84a6FA593eC0898E979eB926Db5b64C2

Network
Goerli **TESTNET**

Language
Solidity

Deployment Date
May 20, 2023

Verified?
Yes

Total Supply
10,000,000,000,000

Status
Not launched

TAXES

Buy Tax
7%

Sell Tax
7%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of May 24, 2023)

Liquidity

Not added yet

Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
500,000,000,000

LP Address(es)

Liquidity not added yet

03

TOKEN TRANSFERS STATS

Transfer Count	TESTNET
Uniq Senders	TESTNET
Uniq Receivers	TESTNET
Total Amount	TESTNET
Median Transfer Amount	TESTNET
Average Transfer Amount	TESTNET
First transfer date	TESTNET
Last transfer date	TESTNET
Days token transferred	TESTNET

SMART CONTRACT STATS

Calls Count	TESTNET
External calls	TESTNET
Internal calls	TESTNET
Transactions count	TESTNET
Uniq Callers	TESTNET
Days contract called	TESTNET
Last transaction time	TESTNET
Created	TESTNET
Create TX	TESTNET
Creator	TESTNET

FEATURED WALLETS

Owner address	TESTNET
Marketing fee receiver	TESTNET
LP address	TESTNET

TOP 3 UNLOCKED WALLETS

1
N/A

2
N/A

3
N/A
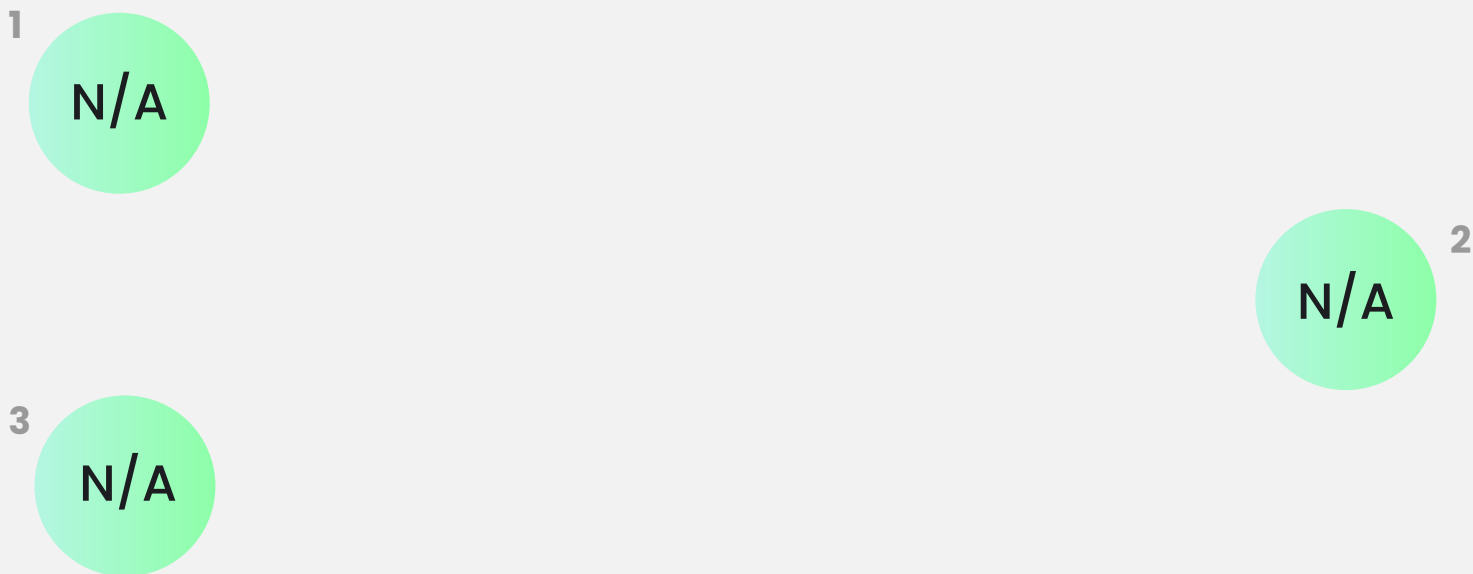
VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

06

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

07

⚠️ Medium Risk

Owner can set buy fees up to 20% and sell fees up to 25%.
Combined buy+sell = 45%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```solidity
function updateBuyFees(uint256 _marketingFee, uint256 _liquidityFee,
uint256 _buyBackFee, uint256 _devFee) external onlyOwner {
    buyMarketingFee = _marketingFee;
    buyLiquidityFee = _liquidityFee;
    buyBuyBackFee = _buyBackFee;
    buyDevFee = _devFee;
    buyTotalFees = buyMarketingFee + buyLiquidityFee + buyBuyBackFee + buyDevFee;
    require(buyTotalFees <= 20, "Must keep fees at 20% or less");
}

function updateSellFees(uint256 _marketingFee, uint256 _liquidityFee,
uint256 _buyBackFee, uint256 _devFee) external onlyOwner {
    sellMarketingFee = _marketingFee;
    sellLiquidityFee = _liquidityFee;
    sellBuyBackFee = _buyBackFee;
    sellDevFee = _devFee;
    sellTotalFees = sellMarketingFee + sellLiquidityFee + sellBuyBackFee + sellDevFee;
    require(sellTotalFees <= 25, "Must keep fees at 25% or less");
}
```

- Recommendation:
  - Considered as good tax deduction pracice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠️ Medium Risk

Owner can burn up to 10% of the liquidity pair's tokens supply.
When tokens are burnt from liquidity pair, price per token will increase.
This can be abused by large token holders.

```solidity
uint256 public manualBurnFrequency = 1 hours;
function manualBurnLiquidityPairTokens(uint256 percent) external onlyOwner {
    require(block.timestamp > lastManualLpBurnTime + manualBurnFrequency , "Must wait for cooldown to finish");
    require(percent <= 1000, "May not nuke more than 10% of tokens in LP");
    lastManualLpBurnTime = block.timestamp;

    // get balance of liquidity pair
    uint256 liquidityPairBalance = this.balanceOf(lpPair);

    // calculate amount to burn
    uint256 amountToBurn = liquidityPairBalance * percent / 10000;

    if (amountToBurn > 0){
        super._transfer(lpPair, address(0xdead), amountToBurn);
    }

    //sync price since this is not in a swap transaction!
    IDexPair pair = IDexPair(lpPair);
    pair.sync();
    emit ManualNukeLP(amountToBurn);
}
```

- Recommendation:
  - Tokens should not be burnt from the liquidity pair.

08-C

ℹ️ Informational

Owner can exclude address from fees.
Owner can exclude address from max transaction limit.

```solidity
function excludeFromMaxTransaction(address updAds, bool isEx) public onlyOwner {
    _isExcludedmaxTxnAmount[updAds] = isEx;
}

function excludeFromFees(address account, bool excluded) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

Owner can set max transaction limit but cannot lower it than 0.5% of total supply.

```solidity
function updateMaxTxnAmount(uint256 newNum) external onlyOwner {
    require(newNum >= (totalSupply() * 5 / 1000)/1e18,
    "Cannot set maxTxnAmount lower than 0.5%");
    maxTxnAmount = newNum * (10**18);
}
```

Owner can set max transaction limit but cannot lower it than 0.5% of total supply.

```solidity
function setAutoLPBurnSettings(uint256 _frequencyInSeconds,
uint256 _percent, bool _Enabled) external onlyOwner {
    require(_frequencyInSeconds >= 600, "cannot set buyback more often than every
    require(_percent <= 1000 && _percent >= 0, "Must set auto LP burn percent bet
    lpBurnFrequency = _frequencyInSeconds;
    percentForLPBurn = _percent;
    lpBurnEnabled = _Enabled;
}

function _transfer(address from, address to, uint256 amount) internal override {
    ...........................
    if(!swapping && automatedMarketMakerPairs[to] && lpBurnEnabled &&
    block.timestamp >= lastLpBurnTime + lpBurnFrequency && !_isExcludedFromFees[from]
        autoBurnLiquidityPairTokens();
}
    ...........................
}

function autoBurnLiquidityPairTokens() internal{

    lastLpBurnTime = block.timestamp;

    // get balance of liquidity pair
    uint256 liquidityPairBalance = this.balanceOf(lpPair);

    // calculate amount to burn
    uint256 amountToBurn = liquidityPairBalance * percentForLPBurn / 10000;
```

SPYWOLF.CO

ℹ️ Informational

Initial liquidity should be added and token should be launched via the launch() function.

```solidity
function launch(uint256 _blockPenalty) external onlyOwner {
    require(!tradingActive, "Trading is already active, cannot relaunch.");

    blockPenalty = _blockPenalty;
    //update name/ticker
    _name = "BLOOMBLOCK";
    _symbol = "BLOOM";

    //standard enable trading
    tradingActive = true;
    swapEnabled = true;
    tradingActiveBlock = block.number;
    lastLpBurnTime = block.timestamp;
    // initialize router
    IDexRouter _dexRouter = IDexRouter(0xD99D1c33F9fC3444f8101754aBC46c52416550D1);
    dexRouter = _dexRouter;
    // create pair
    lpPair = IDexFactory(_dexRouter.factory()).createPair(address(this), _dexRouter.WETH());
    excludeFromMaxTransaction(address(lpPair), true);
    _setAutomatedMarketMakerPair(address(lpPair), true);

    // add the liquidity
    require(address(this).balance > 0, "Must have ETH on contract to launch");
    require(balanceOf(address(this)) > 0, "Must have Tokens on contract to launch");
    _approve(address(this), address(dexRouter), balanceOf(address(this)));
    dexRouter.addLiquidityETH{value: address(this).balance}(
        address(this),
        balanceOf(address(this)),
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        0xaf497A158fC47F2Dee27c4C560ae6a192168983F,
        block.timestamp
    );
}
```

08-E

RECOMMENDATIONS FOR

GOOD PRACTICES

1	Consider fundamental tradeoffs
2	Be attentive to blockchain properties
3	Ensure careful rollouts
4	Keep contracts simple
5	Stay up to date and track development

BLOOMBLOCK
GOOD PRACTICES FOUND

✔ The owner cannot mint new tokens after deployment

✔ The owner cannot stop or pause the contract

✔ The owner can set a transaction limit, but can't lower it than 0.5% of total supply

09

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

✔ **OVER 150 SUCCESSFUL CLIENTS**

✔ **MORE THAN 500 SCAMS EXPOSED**

✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

🌐 **SPYWOLF.NETWORK**

✈ **@SPYWOLFNETWORK**

✈ **@SPYWOLFOFFICIAL**

🐦 **@SPYWOLFNETWORK**

@SPYWOLFNETWORK

10

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.